CLAIMS

What is claimed is:

1. A computing device for securely executing authorized code, said computing device comprising:

a protected memory for storing authorized code, which contains an original digital signature; and

a processor in signal communication with said protected memory for preparing to execute code from the protected memory by verifying that a digital signature contained in said code is original in accordance with a public key, and if said original digital signature is verified, then branching to a copy of said authorized code in said protected memory to begin execution.

2. A computing device as recited in Claim 1 wherein said protected memory is cryptographically protected.

3. A computing device as recited in Claim 1 wherein the integrity of the contents of said protected memory is protected by encryption.

4. A computing device as recited in Claim 1 wherein said protected

memory is physically protected.

5. A computing device as recited in Claim 1 wherein said public key is stored in said protected memory.

6. A computing device as recited in Claim 1 wherein at least one of the integrity of said authorized code and the privacy of said authorized code is protected at run time.

7. A computing device as recited in Claim 6 wherein the integrity of said authorized code is protected at run time with symmetric key encryption.

8. A computing device as recited in Claim 6, wherein the privacy of said authorized code is protected at run time with symmetric key encryption.

9. A computing device as defined in Claim 1 wherein:

the protected memory stores code with an original digital signature corresponding to an Owner Public Key; and

the processor verifies the Owner Public Key in accordance with a Manufacturer Public Key, which is resident on the processor, and then

verifies the original digital signature in accordance with the Owner Public Key.

10. A computing device as defined in Claim 9, further comprising:

reading means for reading a Certificate containing an Owner Public Key;

validation means for validating the Certificate with the Manufacturer Public Key;

matching means for finding the Owner Public Key in the Certificate that matches the Owner Number in the processor; and

verification means for using the matched Owner Public Key to verify the authorized code.

11. A method for ensuring that a processor will execute only authorized code, said method comprising:

applying an original digital signature to all authorized code;

storing said signed authorized code in a protected memory;

preparing to execute code from the protected memory by verifying a digital signature used to sign said code in accordance with a public key, which corresponds to said original digital signature; and

if said original digital signature is verified, then branching to a copy of

said authorized code in said protected memory to begin execution.

12. A method as recited in Claim 11 wherein said protected memory is cryptographically protected.

13. A method as recited in Claim 11 wherein the integrity of the contents of said protected memory is protected by encryption.

14. A method as recited in Claim 11 wherein said protected memory is physically protected.

15. A method as recited in Claim 11 wherein said public key is stored in said protected memory.

16. A method as recited in Claim 11 wherein the integrity of said authorized code is protected at run time.

17. A method as recited in Claim 16 wherein the integrity of said authorized code is protected with symmetric key encryption.

18. A method as recited in Claim 11 wherein the privacy of said authorized code is protected at run time.

19. A method as recited in Claim 18 wherein the privacy of said authorized code is protected at run time with symmetric key encryption.

20. A method as defined in Claim 11, further comprising:

storing code in the protected memory with an original digital signature corresponding to an Owner Public Key; and

verifying the Owner Public Key in accordance with a Manufacturer Public Key, which is resident on the processor, and then verifying the original digital signature in accordance with the Owner Public Key.

21. A method as defined in Claim 20, further comprising:

reading a Certificate containing an Owner Public Key;

validating the Certificate with the Manufacturer Public Key;

finding the Owner Public Key in the Certificate that matches the Owner Number in the processor; and

using the matched Owner Public Key to verify the authorized code.

22. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform program steps for ensuring that a processor will execute only authorized code, the program steps comprising:

applying an original digital signature to all authorized code;

storing said signed authorized code in a protected memory;

preparing to execute code from the protected memory by verifying a digital signature used to sign said code in accordance with a public key, which corresponds to said original digital signature; and

branching to a copy of said authorized code in said protected memory to begin execution if said original digital signature is verified.